

**Congress of the United States**  
**House of Representatives**  
**Washington, D.C. 20515**

**528**

June 26, 2017

The Honorable Ajit V. Pai  
Chairman  
Federal Communications Commission  
445 12th Street SW  
Washington, D.C. 20554

The Honorable Mignon L. Clyburn  
Commissioner  
Federal Communications Commission  
445 12th Street SW  
Washington, D.C. 20554

The Honorable Michael O’Rielly  
Commissioner  
Federal Communications Commission  
445 12th Street SW  
Washington, D.C. 20554

Dear Chairman Pai, Commissioner Clyburn, and Commissioner O’Rielly:

We write to express concerns about the Federal Communications Commission’s (FCC) cybersecurity preparedness, and the multiple reported problems with the FCC’s website in taking public comments in the net neutrality proceeding. Recent events have raised questions about the security of the FCC’s network, and we have serious concerns that the FCC’s website failures deprive the public of opportunities to comment on net neutrality – an issue that affects everyone who uses the internet.

Problems with the FCC’s net neutrality docket made headlines last month after comedian John Oliver implored his viewers to file comments about net neutrality with the FCC. Multiple media outlets reported that the FCC’s Electronic Comment Filing System “went down”<sup>1</sup> after the segment, noting that “the FCC’s servers appeared to be overwhelmed by the flood of traffic.”<sup>2</sup>

The following day, on May 8, 2017, the FCC’s Chief Information Officer announced that the FCC “was subject to multiple distributed denial-of-service attacks,” a situation that made it

---

<sup>1</sup> Ali Breland, *FCC site crashes after John Oliver segment*, The Hill (May 8, 2017). See also, Sam Gustin, *John Oliver Just Crashed the FCC’s Website Over Net Neutrality—Again*, Motherboard (May 8, 2017).

<sup>2</sup> Jeff John Roberts, *John Oliver Gets Fired Up Over Net Neutrality—and FCC’s Site Goes Down*, Fortune (May 8, 2017).

“difficult for legitimate commenters to access and file with the FCC.”<sup>3</sup> In response to an inquiry from Senators Wyden and Schatz, the FCC recently released more information about the alleged cyberattacks.<sup>4</sup> Yet the FCC’s response raises additional questions, and there are other areas of concern about the net neutrality docket for which we seek answers.

For example, recent reports have also indicated that as many as 150,000 comments had disappeared from the FCC’s net neutrality docket,<sup>5</sup> and that automated comments were submitted to the FCC using names and addresses of real people without their knowledge or consent.<sup>6</sup> Even with all of these problems and irregularities, the FCC has given only until the middle of August for the public to provide initial comments on the FCC’s net neutrality proposal, despite receiving calls to extend the deadline.<sup>7</sup> Further, Republican Congressional leaders have not held hearings to examine these issues, despite receiving calls to do so.<sup>8</sup>

We ask you to examine these serious problems and irregularities that raise doubts about the fairness, and perhaps even the legitimacy, of the FCC’s process in its net neutrality proceeding. Giving the public an opportunity to comment in an open proceeding such as this one is crucial – so that the FCC can consider the full impact of its proposals, and treat everyone who would be affected fairly. It is also required by law. The FCC must comply with Administrative

---

<sup>3</sup> Federal Communications Commission, *FCC CIO Statement on Distributed Denial-of-Service Attacks on FCC Electronic Comment Filing System* (May 8, 2017) (press release).

<sup>4</sup> Letter from Ajit V. Pai, Chairman, Federal Communications Commission, to Senators Wyden and Schatz (June 15, 2017) (<https://www.politicopro.com/f/?id=0000015c-d59b-de74-a17f-ddbba4380001>) (FCC Response).

<sup>5</sup> John Eggerton, *FCC’s Network Neutrality Docket Appears to Shrink*, *Broadcasting & Cable* (June 8, 2017).

<sup>6</sup> Dominic Rushe, *‘Pretty ridiculous’: thousands of names stolen to attack net neutrality rules*, *The Guardian* (May 26, 2017).

<sup>7</sup> Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, and Rep. Mike Doyle, Ranking Member, Subcommittee on Communications and Technology, House Committee on Energy and Commerce, to Ajit V. Pai, Chairman, Federal Communications Commission (May 11, 2017).

<sup>8</sup> Letter from Rep. Frank Pallone, Jr., Ranking Member, House Committee on Energy and Commerce, Rep. Diana DeGette, Ranking Member, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, Rep. Mike Doyle, Ranking Member, Subcommittee on Communications and Technology, House Committee on Energy and Commerce, and Yvette Clarke, Member of Congress, to Rep. Greg Walden, Chairman, House Committee on Energy and Commerce, Rep. Tim Murphy, Chairman, Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce, and Rep. Marsha Blackburn, Chairman, Subcommittee on Communications and Technology, House Committee on Energy and Commerce (May 17, 2017).

Procedure Act requirements to give the public notice and an opportunity to comment, as well as to respond to those comments.<sup>9</sup> This is important, especially where the FCC is considering changing rules that affect everyone who uses the internet.

It is also critical that the FCC take all appropriate measures to secure its networks from cyberattacks. At a minimum, the FCC must meet cybersecurity requirements under the Federal Information Security Modernization Act (FISMA). The Chairman of the FCC is ultimately responsible under FISMA to provide information security protections for the agency.<sup>10</sup> This is especially important given that the FCC’s Chief Information Officer stated that the FCC experienced a cyberattack that made it difficult for members of the public to file comments with the agency in an open proceeding.<sup>11</sup> We therefore request responses to the following questions by July 17, 2017:

1. According to the FCC’s response to Senators Wyden and Schatz, the May 2017 incident was a “non-traditional DDoS attack” where bot traffic “increased exponentially” between 11pm EST on May 7, 2017 until 1pm EST on May 8, 2017, representing a “3,000% increase in normal volume.”<sup>12</sup> What “additional solutions” is the FCC pursuing to “further protect the system,” as was mentioned in the FCC’s response?<sup>13</sup>
2. According to the FCC, the alleged cyberattacks blocked “new human visitors.... from visiting the comment filing system.”<sup>14</sup> Yet, the FCC, consulting with the FBI, determined that “the attack did not rise to the level of a major incident that would trigger further FBI involvement.”<sup>15</sup> What analysis did the FCC and the FBI conduct to determine that this was not a “major incident?”

---

<sup>9</sup> 5 U.S.C. § 553. *See, e.g., Am. Radio Relay League, Inc. v. FCC*, 524 F.3d 227 (D.C. Cir) (2007) (remanding final rule to the FCC after finding the FCC had failed to comply with obligation under the Administrative Procedure Act to give interested parties notice and a reasonable opportunity to comment in the rulemaking process); *Home Box Office, Inc. v. FCC*, 567 F.2d 9 (D.C. Cir.) (1977) (vacating rule for failure of the FCC to comply with the Administrative Procedure Act’s notice and comment requirements that are intended to “provide fair treatment for persons affected by a rule.”).

<sup>10</sup> 44 U.S.C. § 3554(a).

<sup>11</sup> FCC Press Release, *supra* n. 3.

<sup>12</sup> FCC Response, *supra* n. 4.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*

<sup>15</sup> *Id.*



The Honorable Ajit V. Pai  
The Honorable Mignon L. Clyburn  
The Honorable Michael O'Rielly  
June 26, 2017  
Page 4

3. What specific "hardware resources" will the FCC commit to accommodate people attempting to file comments during high-profile proceedings? Does the FCC have sufficient resources for that purpose?
4. Is the FCC making alternative ways available for members of the public to file comments in the net neutrality proceeding?
5. Did the FCC contact the National Cybersecurity and Communications Integration Center's Hunt and Incident Response Team (HIRT) at the U.S. Department of Homeland Security to investigate the May 8, 2017 incident, and if so, on which date(s) was such contact made? If the FCC did not contact HIRT to investigate the May 8, 2017 incident, please explain why it did not do so.
6. What were the findings from any forensic investigative analyses or reports concerning the May 8, 2017 incident, including how and why a denial-of-service attacks were declared, and from what attack vectors they came?
7. Did the FCC notify Congress of the May 8, 2017 incidents as provided by FISMA?<sup>16</sup> If so, how did the FCC notify Congress? If not, why not?
8. Did the FCC notify its Office of Inspector General (OIG) of the May 8, 2017 incidents, and if so, when did it notify the OIG?

Your assistance in this matter is greatly appreciated, and we look forward to receiving a response. If you have any questions, please contact the minority committee staff of the House Energy and Commerce Committee at (202) 225-3641 and the minority committee staff of the House Oversight and Government Reform Committee at (202) 225-5051.

Sincerely,



Frank Pallone, Jr.  
Ranking Member  
Committee on Energy  
and Commerce



Elijah E. Cummings  
Ranking Member  
Committee on Oversight  
and Government Reform

---

<sup>16</sup> 44 U.S.C. § 3554(b)(7)(C)(iii)(III).



The Honorable Ajit V. Pai  
The Honorable Mignon L. Clyburn  
The Honorable Michael O'Rielly  
June 26, 2017  
Page 5



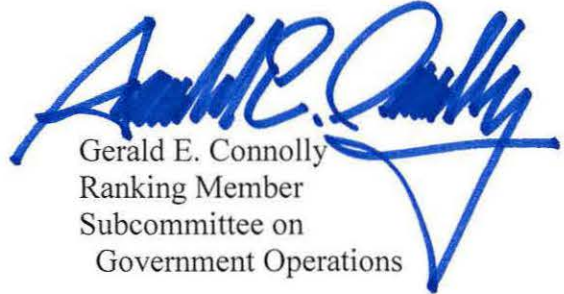
Diana DeGette  
Ranking Member  
Subcommittee on Oversight and  
Investigations



Robin L. Kelly  
Ranking Member  
Subcommittee on  
Information Technology



Mike Doyle  
Ranking Member  
Subcommittee on Communications  
and Technology



Gerald E. Connolly  
Ranking Member  
Subcommittee on  
Government Operations

Cc: The Honorable Trey Gowdy, Chairman  
House Committee on Oversight and Government Reform

The Honorable Greg Walden, Chairman  
House Committee on Energy and Commerce





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 21, 2017

OFFICE OF  
THE CHAIRMAN

The Honorable Gerald Connolly  
Ranking Member  
Subcommittee on Government Operations  
Committee on Oversight and Government Reform  
U.S. House of Representatives  
2238 Rayburn House Office Building  
Washington, D.C. 20515

Dear Congressman Connolly:

Thank you for your June 26, 2017 letter and questions concerning the Federal Communications Commission's (FCC's or Commission's) cybersecurity preparedness and its impact on the FCC's ability to accept comments from the public in ongoing proceedings.

I consider any disruption of the FCC's systems by outside parties to be a very serious matter. That's why our Information Technology (IT) staff immediately addressed the disruption to the FCC's Electronic Comment Filing System (ECFS) that began late in the evening on May 7 and mitigated the impact on filers by the morning of the following day, May 8. And following the events of May 7-8, I directed our Chief Information Officer (CIO) to take appropriate measures to continue securing the comment filing system and to report back to my staff routinely on this work. I also directed the CIO to fully assist in any official inquiries related this matter and to comply with all applicable federal guidelines and laws governing such incidents.

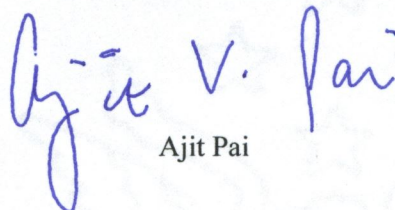
This work was successful and from Monday, May 8 to Friday, May 12, we received more than 2.1 million comments. To put this number in perspective, the FCC usually averages 10,000 comments per day in total for all our proceedings combined.

Moreover, during the past two months, the Commission's IT staff has taken additional steps to prevent potential disruptions similar to the May 7-8 event as well as to ensure the ongoing integrity and resiliency of the system. And ECFS has performed well during the comment period following the adoption of the *Restoring Internet Freedom Notice of Proposed Rulemaking*. The docket now contains more than 10 million comments overall, demonstrating that our processes are facilitating widespread public participation in this proceeding. Indeed, the system did not experience any difficulties in the leadup to the deadline for initial comments, which was earlier this week.

Although I cannot guarantee that we will not experience further attempts to disrupt our systems, our staff is constantly monitoring and reviewing the situation so that that everyone seeking to comment on our proceedings will be afforded the opportunity to do so. We are committed to this goal and will continue to foster a transparent process that encourages public participation in our proceedings.

The CIO has provided me with the attached answers to the list of questions in your letter. Please let me know if I can be of any further assistance.

Sincerely,

  
Ajit Pai

Enclosure





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 21, 2017

OFFICE OF  
THE CHAIRMAN

The Honorable Frank Pallone  
Ranking Member  
Committee on Energy and Commerce  
U.S. House of Representatives  
2125 Rayburn House Office Building  
Washington, D.C. 20515

Dear Congressman Pallone:

Thank you for your June 26, 2017 letter and questions concerning the Federal Communications Commission's (FCC's or Commission's) cybersecurity preparedness and its impact on the FCC's ability to accept comments from the public in ongoing proceedings.

I consider any disruption of the FCC's systems by outside parties to be a very serious matter. That's why our Information Technology (IT) staff immediately addressed the disruption to the FCC's Electronic Comment Filing System (ECFS) that began late in the evening on May 7 and mitigated the impact on filers by the morning of the following day, May 8. And following the events of May 7-8, I directed our Chief Information Officer (CIO) to take appropriate measures to continue securing the comment filing system and to report back to my staff routinely on this work. I also directed the CIO to fully assist in any official inquiries related this matter and to comply with all applicable federal guidelines and laws governing such incidents.

This work was successful and from Monday, May 8 to Friday, May 12, we received more than 2.1 million comments. To put this number in perspective, the FCC usually averages 10,000 comments per day in total for all our proceedings combined.

Moreover, during the past two months, the Commission's IT staff has taken additional steps to prevent potential disruptions similar to the May 7-8 event as well as to ensure the ongoing integrity and resiliency of the system. And ECFS has performed well during the comment period following the adoption of the *Restoring Internet Freedom Notice of Proposed Rulemaking*. The docket now contains more than 10 million comments overall, demonstrating that our processes are facilitating widespread public participation in this proceeding. Indeed, the system did not experience any difficulties in the leadup to the deadline for initial comments, which was earlier this week.

Although I cannot guarantee that we will not experience further attempts to disrupt our systems, our staff is constantly monitoring and reviewing the situation so that that everyone seeking to comment on our proceedings will be afforded the opportunity to do so. We are committed to this goal and will continue to foster a transparent process that encourages public participation in our proceedings.

The CIO has provided me with the attached answers to the list of questions in your letter. Please let me know if I can be of any further assistance.

Sincerely,

Ajit Pai

Enclosure





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 21, 2017

OFFICE OF  
THE CHAIRMAN

The Honorable Elijah Cummings  
Ranking Member  
Committee on Oversight and Government Reform  
U.S. House of Representatives  
2163 Rayburn House Office Building  
Washington, D.C. 20515

Dear Congressman Cummings:

Thank you for your June 26, 2017 letter and questions concerning the Federal Communications Commission's (FCC's or Commission's) cybersecurity preparedness and its impact on the FCC's ability to accept comments from the public in ongoing proceedings.

I consider any disruption of the FCC's systems by outside parties to be a very serious matter. That's why our Information Technology (IT) staff immediately addressed the disruption to the FCC's Electronic Comment Filing System (ECFS) that began late in the evening on May 7 and mitigated the impact on filers by the morning of the following day, May 8. And following the events of May 7-8, I directed our Chief Information Officer (CIO) to take appropriate measures to continue securing the comment filing system and to report back to my staff routinely on this work. I also directed the CIO to fully assist in any official inquiries related this matter and to comply with all applicable federal guidelines and laws governing such incidents.

This work was successful and from Monday, May 8 to Friday, May 12, we received more than 2.1 million comments. To put this number in perspective, the FCC usually averages 10,000 comments per day in total for all our proceedings combined.

Moreover, during the past two months, the Commission's IT staff has taken additional steps to prevent potential disruptions similar to the May 7-8 event as well as to ensure the ongoing integrity and resiliency of the system. And ECFS has performed well during the comment period following the adoption of the *Restoring Internet Freedom Notice of Proposed Rulemaking*. The docket now contains more than 10 million comments overall, demonstrating that our processes are facilitating widespread public participation in this proceeding. Indeed, the system did not experience any difficulties in the leadup to the deadline for initial comments, which was earlier this week.

Although I cannot guarantee that we will not experience further attempts to disrupt our systems, our staff is constantly monitoring and reviewing the situation so that that everyone seeking to comment on our proceedings will be afforded the opportunity to do so. We are committed to this goal and will continue to foster a transparent process that encourages public participation in our proceedings.

The CIO has provided me with the attached answers to the list of questions in your letter. Please let me know if I can be of any further assistance.

Sincerely,

Ajit Pai

Enclosure





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 21, 2017

OFFICE OF  
THE CHAIRMAN

The Honorable Diana DeGette  
Ranking Member  
Subcommittee on Oversight and Investigations  
Committee on Energy and Commerce  
U.S. House of Representatives  
2111 Rayburn House Office Building  
Washington, D.C. 20515

Dear Congresswoman DeGette:

Thank you for your June 26, 2017 letter and questions concerning the Federal Communications Commission's (FCC's or Commission's) cybersecurity preparedness and its impact on the FCC's ability to accept comments from the public in ongoing proceedings.

I consider any disruption of the FCC's systems by outside parties to be a very serious matter. That's why our Information Technology (IT) staff immediately addressed the disruption to the FCC's Electronic Comment Filing System (ECFS) that began late in the evening on May 7 and mitigated the impact on filers by the morning of the following day, May 8. And following the events of May 7-8, I directed our Chief Information Officer (CIO) to take appropriate measures to continue securing the comment filing system and to report back to my staff routinely on this work. I also directed the CIO to fully assist in any official inquiries related this matter and to comply with all applicable federal guidelines and laws governing such incidents.

This work was successful and from Monday, May 8 to Friday, May 12, we received more than 2.1 million comments. To put this number in perspective, the FCC usually averages 10,000 comments per day in total for all our proceedings combined.

Moreover, during the past two months, the Commission's IT staff has taken additional steps to prevent potential disruptions similar to the May 7-8 event as well as to ensure the ongoing integrity and resiliency of the system. And ECFS has performed well during the comment period following the adoption of the *Restoring Internet Freedom Notice of Proposed Rulemaking*. The docket now contains more than 10 million comments overall, demonstrating that our processes are facilitating widespread public participation in this proceeding. Indeed, the system did not experience any difficulties in the leadup to the deadline for initial comments, which was earlier this week.

Although I cannot guarantee that we will not experience further attempts to disrupt our systems, our staff is constantly monitoring and reviewing the situation so that that everyone seeking to comment on our proceedings will be afforded the opportunity to do so. We are committed to this goal and will continue to foster a transparent process that encourages public participation in our proceedings.

The CIO has provided me with the attached answers to the list of questions in your letter. Please let me know if I can be of any further assistance.

Sincerely,

Ajit Pai

Enclosure





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 21, 2017

OFFICE OF  
THE CHAIRMAN

The Honorable Robin Kelly  
Ranking Member  
Subcommittee on Information Technology  
Committee on Oversight and Government Reform  
U.S. House of Representatives  
1239 Longworth House Office Building  
Washington, D.C. 20515

Dear Congresswoman Kelly:

Thank you for your June 26, 2017 letter and questions concerning the Federal Communications Commission's (FCC's or Commission's) cybersecurity preparedness and its impact on the FCC's ability to accept comments from the public in ongoing proceedings.

I consider any disruption of the FCC's systems by outside parties to be a very serious matter. That's why our Information Technology (IT) staff immediately addressed the disruption to the FCC's Electronic Comment Filing System (ECFS) that began late in the evening on May 7 and mitigated the impact on filers by the morning of the following day, May 8. And following the events of May 7-8, I directed our Chief Information Officer (CIO) to take appropriate measures to continue securing the comment filing system and to report back to my staff routinely on this work. I also directed the CIO to fully assist in any official inquiries related this matter and to comply with all applicable federal guidelines and laws governing such incidents.

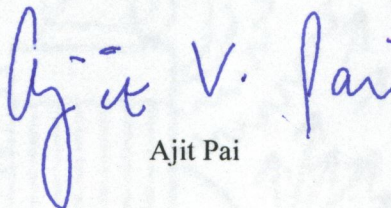
This work was successful and from Monday, May 8 to Friday, May 12, we received more than 2.1 million comments. To put this number in perspective, the FCC usually averages 10,000 comments per day in total for all our proceedings combined.

Moreover, during the past two months, the Commission's IT staff has taken additional steps to prevent potential disruptions similar to the May 7-8 event as well as to ensure the ongoing integrity and resiliency of the system. And ECFS has performed well during the comment period following the adoption of the *Restoring Internet Freedom Notice of Proposed Rulemaking*. The docket now contains more than 10 million comments overall, demonstrating that our processes are facilitating widespread public participation in this proceeding. Indeed, the system did not experience any difficulties in the leadup to the deadline for initial comments, which was earlier this week.

Although I cannot guarantee that we will not experience further attempts to disrupt our systems, our staff is constantly monitoring and reviewing the situation so that that everyone seeking to comment on our proceedings will be afforded the opportunity to do so. We are committed to this goal and will continue to foster a transparent process that encourages public participation in our proceedings.

The CIO has provided me with the attached answers to the list of questions in your letter. Please let me know if I can be of any further assistance.

Sincerely,



Ajit Pai

Enclosure





FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON

July 21, 2017

OFFICE OF  
THE CHAIRMAN

The Honorable Mike Doyle  
Ranking Member  
Subcommittee on Communications and Technology  
Committee on Energy and Commerce  
U.S. House of Representatives  
239 Cannon House Office Building  
Washington, D.C. 20515

Dear Congressman Doyle:

Thank you for your June 26, 2017 letter and questions concerning the Federal Communications Commission's (FCC's or Commission's) cybersecurity preparedness and its impact on the FCC's ability to accept comments from the public in ongoing proceedings.

I consider any disruption of the FCC's systems by outside parties to be a very serious matter. That's why our Information Technology (IT) staff immediately addressed the disruption to the FCC's Electronic Comment Filing System (ECFS) that began late in the evening on May 7 and mitigated the impact on filers by the morning of the following day, May 8. And following the events of May 7-8, I directed our Chief Information Officer (CIO) to take appropriate measures to continue securing the comment filing system and to report back to my staff routinely on this work. I also directed the CIO to fully assist in any official inquiries related this matter and to comply with all applicable federal guidelines and laws governing such incidents.

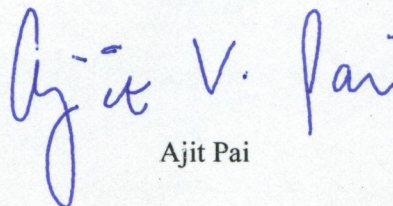
This work was successful and from Monday, May 8 to Friday, May 12, we received more than 2.1 million comments. To put this number in perspective, the FCC usually averages 10,000 comments per day in total for all our proceedings combined.

Moreover, during the past two months, the Commission's IT staff has taken additional steps to prevent potential disruptions similar to the May 7-8 event as well as to ensure the ongoing integrity and resiliency of the system. And ECFS has performed well during the comment period following the adoption of the *Restoring Internet Freedom Notice of Proposed Rulemaking*. The docket now contains more than 10 million comments overall, demonstrating that our processes are facilitating widespread public participation in this proceeding. Indeed, the system did not experience any difficulties in the leadup to the deadline for initial comments, which was earlier this week.

Although I cannot guarantee that we will not experience further attempts to disrupt our systems, our staff is constantly monitoring and reviewing the situation so that that everyone seeking to comment on our proceedings will be afforded the opportunity to do so. We are committed to this goal and will continue to foster a transparent process that encourages public participation in our proceedings.

The CIO has provided me with the attached answers to the list of questions in your letter. Please let me know if I can be of any further assistance.

Sincerely,



Ajit Pai

Enclosure



1. **According to the FCC's response to Senators Wyden and Schatz, the May 2017 incident was a "non-traditional DDoS attack" where bot traffic "increased exponentially" between 11pm EST on May 7, 2017 until 1pm EST on May 8, 2017, representing a "3,000% increase in normal volume." What "additional solutions" is the FCC pursuing to "further protect the system," as mentioned in the FCC's response?**

First, for your records, please note the following correction to your question above concerning the timing of this event. As we stated in our earlier response to Senators Wyden and Schatz, bot traffic increased exponentially from 11:00 p.m. to 1:00 a.m., EST – not 1:00 p.m. We provided this timeline to assist in understanding the nature of the attack.

Given the ongoing nature of the threats to disrupt the Commission's electronic comment filing system, it would undermine our system's security to provide a specific roadmap of the additional solutions to which we have referred. However, we can state that the FCC's IT staff has worked with commercial cloud providers to implement internet-based solutions to limit the amount of disruptive bot-related activity if another bot-driven event occurs.

The FCC also instituted a more predictive model for assessing the number of incoming comments and bot driven activity to ensure we will have more cloud-based resources available within a shorter time period to respond to potential surges in activity. In addition, the FCC implemented a control feature that recognizes when there is heavy bot traffic. This improvement allows humans (as opposed to bots) to continue to access the electronic comment filing system even if a large amount of bot activity is also present.

2. **According to the FCC, the alleged cyberattacks blocked "new human visitors . . . from visiting the comment filing system." Yet, the FCC, consulting with the FBI, determined that "the attack did not rise to the level of a major incident that would trigger further FBI involvement." What analysis did the FCC and the FBI conduct to determine that this was not a "major incident?"**

The FCC consulted with the FBI following this incident, and it was agreed this was not a "significant cyber incident" consistent with the definition contained in Presidential Policy Directive-41 (PPD-41). Equally, it is important to note the May 7-8 disruption was not a system "hack" or intrusion and at no point was the Commission's network cybersecurity breached.

3. **What specific "hardware resources" will the FCC commit to accommodate people attempting to file comments during high-profile proceedings? Does the FCC have sufficient resources for that purpose?**

The Commission's Electronic Comment Filing System is commercially cloud-based, so our "hardware resources" are provided by our commercial partners. While it would undermine our system security to provide a specific roadmap of what we are doing, we can state that FCC IT staff has notified its cloud providers of the need to have sufficient "hardware resources" available to accommodate high-profile proceedings. In addition, FCC IT staff has worked with commercial cloud providers to implement internet-based solutions to limit the amount of disruptive bot-related activity if another bot-driven event occurs.



- 4. Is the FCC making alternative ways available for members of the public to file comments in the net neutrality proceeding?**

Yes, filers always have four alternatives for submitting comments: sending a written document, filing through the normal web interface, filing through the API, or submitting through the electronic inbox using the Bulk Upload Template.

- 5. Did the FCC contact the National Cybersecurity and Communication Integration Center's Hunt and Incident Response Team (HIRT) at the U.S. Department of Homeland Security to investigate the May 8th, 2017 incident, and if so, which date(s) was such contact made? If the FCC did not contact HIRT to investigate the May 8th, 2017 incident, please explain why it did not do so.**

The FCC did not contact HIRT because this event was not categorized as a "significant cyber incident" under PPD-41.

- 6. What were the findings from any forensic investigative analyses or reports concerning the May 8th, 2017 incident, including how and why a denial-of-service attacks were declared, and from what attack vectors they came?**

Our response to Senators Wyden and Schatz describes why we have categorized this incident as a non-traditional DDoS attack. Otherwise, the investigation is ongoing at this stage.

- 7. Did the FCC notify Congress of the May 8th, 2017 incidents as provided by FISMA? And if so, how did the FCC notify Congress? If not, why not?**

Although I have been advised that the FCC's Office of Legislative Affairs provided background information on this matter to the committee offices, we did not provide a FISMA-based notification. We determined that this event was not a "major incident" under the Office of Management and Budget's (OMB) definition and hence it did not meet the criteria of a reportable incident to Congress under OMB's FISMA guidance.

Our rationale was based on the OMB guidance on FISMA contained in M-17-05, which provides instructions to agencies on when and how to report a "major incident" to Congress. Under OMB's FISMA guidance, a "major incident" is automatically a "significant cyber incident" per PPD-41, and the definitions of the two terms are closely related. As discussed in the response to question number 2, this event was not categorized as a "significant cyber incident" per PPD-41.

- 8. Did the FCC notify its Office of the Inspector General (OIG) of the May 8th, 2017 incidents, and if so, when did it notify the OIG?**

The Office of the Inspector General contacted FCC's management on May 10, 2017, and we have provided information to them about the incident.